CLAIMS

WHAT IS CLAIMED:

1. A method, comprising:

executing a software object;

establishing a security level for said software object;

performing a virtual address based memory access using at least one of said security levels; and

executing said function of said object based upon said virtual address based memory access.

2. The method described in claim 1, wherein executing a software object further comprises using a processor to process software code of said software object.

3. The method described in claim 1, wherein establishing a security level for said software object further comprises assigning a security level relating to a memory access of at least a portion of a memory.

4. The method described in claim 1, wherein performing said virtual address based memory access using at least one of said security level further comprises:

establishing a secondary table;

receiving a memory access request based upon executing of said software object;

performing said virtual address memory access based upon said memory access request using said secondary table and at least one virtual memory table; and

accessing a portion of a memory based upon said multi-level table access.

5. The method described in claim 4, wherein establishing a secondary table further comprises:

dividing a physical memory into a plurality of segments;

determining at least one of said segment to omit from said secondary table and at least one un-omitted segment;

assigning a default security level to said omitted segment;

assigning a security level to said un-omitted segment; and

correlate at least one assigned segment with a virtual memory location.

6. The method described in claim 4, wherein performing said virtual address memory access based upon said memory access request further comprises:

determining at least one security level that corresponds to a segment in said secondary table;

verifying a match between an execution security level to a security level associated with a segment being accessed in response to an execution of said object;

determining a virtual memory address based upon said secondary table in response to a match between said execution security level and said security level associated with said segment being accessed; and

locating a physical memory location corresponding to a virtual memory address.

7. The method described in claim 6, wherein determining at least one security level that corresponds to said segment in said secondary table further comprises:

determining a physical address from said virtual memory table;

determining a segment being executed based upon said physical address; and

defining a current security level based upon said determining of said segment being executed.

8. A method, comprising:

executing a software object;

establishing a security level for said software object;

establishing a secondary table;

receiving a memory access request based upon said executing of said software object;

determining at least one security level that corresponds to a segment in said secondary table based upon a virtual address; and

accessing a portion of a memory based upon said security level and said virtual address.

9. The method described in claim 8, wherein executing a software object further comprises using a processor to process software code of said software object.

10. The method described in claim 8, wherein establishing a security level for said software object further comprises assigning a security level relating to a memory access of at least a portion of a memory.

11. The method described in claim 8, wherein determining at least one security level that corresponds to a segment in said secondary table comprises:

determining a physical address from said virtual memory table;

determining a segment being executed based upon said physical address; and

defining a current security level based upon said determining of said segment being executed.

12. An apparatus, comprising:

means for executing a software object;

means for establishing a security level for said software object;

means for performing a virtual address based memory access using at least one of said security levels; and

means for executing said function of said object based upon said virtual address based memory access.

13. An apparatus, comprising:

a processor coupled to a bus;

means for coupling at least one software object to said processor;

a memory unit; and

a memory access interface coupled to said bus and said memory unit, said memory access interface to provide said processor a virtual address based access of at least a portion of said memory unit based upon at least one security level, in response to said processor executing said software object.

14. The apparatus of claim 13, wherein said processor comprises at least one microprocessor.

15. The apparatus of claim 13, wherein said memory access interface comprises a virtual memory access table coupled with a secondary table, said memory access interface to provide a virtual memory addressing scheme to access at least one portion of said memory unit based upon a security level.

16. The apparatus of claim 13, wherein said memory unit comprises at least one of a magnetic tape memory, a flash memory, a random access memory, and a memory residing on a semiconductor chip.

17. A computer readable program storage device encoded with instructions that, when executed by a computer, performs a method, comprising:

executing a software object;

establishing a security level for said software object;

performing a virtual address based memory access using at least one of said security levels; and

executing said function of said object based upon said virtual address based memory access.

18. The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 17, wherein executing a software object further comprises using a processor to process software code of said software object.

19. The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 17, wherein establishing a security level for said software object further comprises assigning a security level relating to a memory access of at least a portion of a memory.

20. The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 17, wherein performing a virtual address based memory access using at least one of said security level further comprises:

establishing a secondary table;

receiving a memory access request based upon executing of said software object;

performing a virtual address memory access based upon said memory access request using said secondary table and at least one virtual memory table; and

accessing a portion of a memory based upon said multi-level table access.

21. The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 20, wherein establishing a secondary table further comprises:

dividing a physical memory into a plurality of segments;

determining at least one of said segment to omit from said secondary table and at least one un-omitted segment;

assigning a default security level to said omitted segment;

assigning a security level to said un-omitted segment; and

correlate at least one assigned segment with a virtual memory location.

22. The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 20, wherein performing a virtual address memory access based upon said memory access request further comprises:

determining at least one security level that corresponds to a segment in said secondary table;

verifying a match between an execution security level to a security level associated with a segment being accessed in response to an execution of said object;

determining a virtual memory address based upon said secondary table in response to a match between said execution security level and said security level associated with said segment being accessed; and

locating a physical memory location corresponding to a virtual memory address.

23. The computer readable program storage device encoded with instructions that, when executed by a computer, performs the method described in claim 22, wherein determining at least one security level that corresponds to a segment in said secondary table comprises:

determining a physical address from said virtual memory table;

determining a segment being executed based upon said physical address; and

defining a current security level based upon said determining of said segment being executed.